EU GDPR과 국내 개인정보보호 법제 비교분석★

김 성 현*, 이 창 무**

요 약

2018년 5월 25일부로 시행된 GDPR은 모든 EU 회원국에 공통적으로 적용되고 법적 구속력을 갖춘 점과 개인정보보호와 관련된 가장 최신의 동향이 고려되어진 법이라는 점에서 법적 중요성과 가치가 높다고 할 수 있겠다. 따라서 본 연구는 이러한 GDPR을 기준으로 국내 「개인정보 보호법」 및 「정보통신망법」과의 비교분석을 통한 국내의 개인정보보호 법제의 점검 및 개선 방안을 제언하는 것에 의미가 있을 것이라고 판단하였다. 본 연구의 결과로 GDPR의 법 적용 범위·민감정보 정의·개인정보 이전권·개인정보 보호담당관·개인정보 역외 이전·감독기관·처벌·법 적용 예외 사항 등이 국내 비교대상 법과 차이를 보이고 있었다. 이러한 차이는 정보주체의 권리와 이익을 보호하고, 개인정보의 보호와 활용적 측면의 균형을 위해서도 충분히 필요한 것이었다. 따라서 본 연구의 비교분석 결과 및 법 개선방안에 대한 제언을 토대로 국내 개인정보보호 법제의 전체적인 점검 및 수준 향상에 기여할 수 있을 것으로 기대한다.

A Comparative Analysis of EU GDPR with Privacy Laws in South Korea

Kim Sung Hyun*, Lee Chang Moo**

ABSTRACT

The GDPR implemented since 25 May 2018 is common to all EU Member States and is legally binding. It is also important and legally valuable in that it takes into account the latest trends related to privacy protection. The purpose of this study is to propose a comprehensive review and improvement direction of the personal information protection laws in South Korea through a comparative analysis of EU GDPR and privacy related laws in South Korea. As a result of this study, the differences between the GDPR and privacy related laws in South Korea are Definition of personal sensitive information, Right to data portability, Data protection officer, Transfers of personal data to third countries, Supervisory authority, and Punishment, etc. The differences in these regulations were necessary to protect the rights and interests of data subjects and to properly handle personal information of personal information controllers. Therefore, based on the results of the comparative analysis of this study and suggestions on improvement direction of the law related to personal information protection, it is expected that it will contribute to the overall inspection and improvement of the law related to personal information protection in South Korea.

Key words : EU GDPR, Privacy Laws, Personal Information Protection, Regulation, Comparative Analysis

접수일(2018년 11월 26일), 수정일(1차: 2018년 12월 17일), 게재확정일(2018년 12월 30일)

★ 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터지원사업의 연구결과로 수행되었음. (IITP-2018-2018-0-01799).

* 중앙대학교/일반대학원 산업융합보안학과 (주저자)

** 중앙대학교/경영경제대학 산업보안학과 (교신저자)

1. 서 론

1.1 연구의 필요성 및 목적

오늘날 우리는 정보통신기술의 발달로 빅데이터, 모바일, 인공지능 등의 기술을 이용한 편리하고 고도로 발전된 지능정보사회에서 살아가고 있다. 이러한 환경에서는 방대하고 다양한 정보의 수집과 이에 대한 활발한 활용이 이루어지게 되는데, 그 속에는 필연적으로 개인정보도 포함 될 수밖에 없다. 그러나 개인정보의 경우 본인의 사생활이나 민감할 수 있는 정보도 포함될 수 있기 때문에, 이를 처리할 때는 반드시 적절한 보호조치와 적법한 법을 근거로 이루어져야 한다. 이러한 맥락에서 우리나라를 비롯해 세계 각 국가는 개인정보보호의 중요성을 인지하고 이를 위한 법과 제도, 기술 등을 강화하고 있는 추세이다. 유럽연합(European Union, 이하 'EU') 역시 기존의 개인정보보호지침(Directive 95/46/EC)의 한계를 느끼고, 개인정보에 대한 적절한 보호조치와 이를 뒷받침할 수 있는 합리적인 법과 제도에 대한 필요성을 절감하였다. 이에 그 결과물로서 기존의 개인정보보호지침(Directive 95/46/EC)을 대체하는 '일반정보보호규정'(General Data Protection Regulation, 이하 'GDPR')을 제정 및 시행하게 되었다.

GDPR은 2016년 제정되어 2년간의 유예기간을 거친 뒤 2018년 5월 25일부터 시행된 EU내에서 통용되는 개인정보보호법으로, 이전 1995년 채택되었던 개인정보보호지침(Directive 95/46/EC)을 대체하는 법규범이다. 특히 GDPR은 개인정보보호지침과는 다르게 EU 각 회원국에 직접적으로 적용되며 법적 구속력을 가지고 있다는 점이 특징이다. 또한 2012년 GDPR이 처음 유럽의회에 제안 된 후 4년간의 규정 협의와 같은 EU의 노력과 신중함이 기해진 것은 물론이고, 실제로 법 규정 내용에 있어서도 개인정보와 관련된 최신동향과 필수적인 요소 등이 포함되어 있다[15]. 그렇기 때문에 이러한 GDPR을 분석하고 국내법과 비교분석해 차이점 및 시사점 등을 고찰해본다면, 국내 개인정보보호 관련 법제의 점검은 물론이고, 향후 중요한 입법 참고 자료로도 활용 가능할 것이다. 이에 본 연구는 이러한 시각에서 접근하여 GDPR과 국내 개인정보보호 관련 법률과의 비교분석을 통해 국내 개인정보보호 관련 법제를 점검하고, 필요한 법적 개선점을 도출해봄으로써 국내 개인정보보호 수준 강화에 이바지 하고자 한다.

1.2 연구의 방법 및 범위

본 연구는 EU GDPR과 국내 개인정보보호 관련 법률의 비교분석을 통한 시사점을 도출하고자 하는 것이 주된 내용이기 때문에, 각각의 법 조항 중심으로 비교분석을 진행한다. 비교분석 연구방법은 법률 간의 구체적 규정 내용을 비교해 보고 그 차이점 및 시사점을 고찰하는 방법을 의미한다. 이러한 비교분석 방법이 GDPR과 국내 개인정보보호 관련 법률과의 차이점 및 시사점을 도출하는데 효과적이라는 판단 하에 본 연구의 주된 연구 방법으로 채택하였다. 이에 본 연구는 GDPR의 규정을 중심으로 이와 관련된 규정조항을 국내 비교대상 법률에서 찾아보고 비교분석하여 차이점 및 시사점을 도출해내고자 한다.

비교대상 법으로는 우선 기준이 되는 EU GDPR이 포함되며, 우리나라의 비교 대상 법률로는 「개인정보 보호법」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '「정보통신망법」')」이다. 우선 「개인정보 보호법」은 개인정보보호와 관련 된 일반법이므로 반드시 포함되어야 할 핵심 법률이며, 비교분석 과정 중에서 필요시 세부 규정 확인을 위해 「개인정보 보호법 시행령」 및 지침·기준 등을 참고한다. 다음 「정보통신망법」은 「개인정보 보호법」이 제정되기 이전 「공공기관의 개인정보보호에 관한 법」과 함께 우리나라의 민간영역에 관련된 주요 개인정보보호 규정을 포함한 법률이었다. 현재 「공공기관의 개인정보보호에 관한 법」이 폐지되고 이를 대체하는 「개인정보 보호법」이 제정 및 시행되고 있지만, 여전히 「정보통신망법」은 정보통신서비스 이용자의 개인정보보호와 관련된 상당한 내용을 규정한 채 시행되고 있다. 또한 「정보통신망법」의 개인정보보호 관련 규정은 일반법인 「개인정보 보호법」에 우선하여 적용됨을 제5조(다른 법률과의 관계)에서 밝히고 있기에 개인정보보호와 관련하여 중요한 법률이라고 볼 수 있다. [7]특히 방송통신위원회는 정보통신망(온라인)을 통해 정보를 제공 또는 매개 한다면 업종과 상관없이 정보통신서비스 제공자의 지위에 해

당하고, 결과적으로 「정보통신망법」의 적용을 받는다고 해석하고 있다. 따라서 대부분의 사업자가 「정보통신망법」의 법 적용 대상이 된다는 것을 의미하기에 비교대상 법률로서 채택하였다. 여기서 마찬가지로 비교분석 시 필요한 경우 「정보통신망법 시행령」 및 지침·기준 등을 참고 한다. 이밖에도 다양한 개별 법률에서 일부 개인정보보호와 관련된 내용을 규정하고 있으나, 그 규정 내용이 많지 않고 GDPR 규정 내용과 대응하여 비교분석하기 어렵다고 판단하여 비교대상 법에서 제외하였다. 결과적으로 EU GDPR, 「개인정보 보호법」, 「정보통신망법」 총 3개의 법 규정 내용을 중점적으로 비교분석하여 국내 개인정보보호 법제의 점검 및 시사점을 도출하고자 한다.

2. 이론적 배경 및 선행연구

2.1 EU의 개인정보보호 법제

2.1.1 EU개인정보보호지침(Directive 95/46/EC, 1995)

EU 개인정보보호지침(Data Protection Directive 95/46/EC)은 1995년 제정된 지침(총 7장 34개조)으로, GDPR이 시행되기 전까지 EU의 개인정보보호에 관련한 지침을 규정하고 있었다. 본 지침은 1980년 OECD 프라이버시 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)과 1981년 유럽평의회 협약 108호(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108)에 기초하여 제정되었다[3]. 특히 유럽평의회 협약 108호는 유럽 내에서 처음으로 개인정보보호 분야에 법적 구속력을 가진 규범으로 작용하여 개인정보보호를 개인의 권리로 인정하였다는 점에 그 의의가 있다[3].

EU 개인정보보호지침은 개인정보의 처리와 관련하여 개인의 권리를 규정하고, EU 회원국 간의 동일한 기준을 근거로 자유로운 개인정보의 이동을 보장하려는 지침이었다. 특히 EU가 아닌 제3국으로의 개인정보 이전을 금지하였는데, 제3국이 적정한 수준의 개인정보보호 시스템을 갖춘 경우 예외적으로 이를 허용하였다. 그러나 관리소홀로 인한 제3국의 혹시모를 개인정보 침해사고 등을 우려하여 EU 각 회원국에게 개인정보 보호법제 규정에 대한 방향성을 제시하였다[14]. 이에 따라 영국(Data Protection Act, 1988 제정), 프랑스(Loi n° 78-17 du 6 janvier, 2004년 개정), 독일(BDSG, 2001년 개정) 등은 개인정보보호를 위한 법을 제정 또는 개정 하였다. 따라서 본 지침을 계기로 EU 회원국 간에 동일한 수준의 개인정보 보호가 적용될 수 있었다는데 의의가 있다. 결과적으로 본 지침은 개인정보보호 수준 미달의 국가에 대하여는 정보의 이전을 금지함으로써 EU뿐만 아니라 EU에 속하지 않는 국가의 개인정보보호 정책에도 큰 영향을 미치게 되었고, 전 세계의 개인정보 보호법제의 모델이 되어 왔다[14]. 다만, EU 개인정보보호지침은 '지침'이라는 형식상의 문제로 EU 각 국에 있어 그 규정 조항의 실효성에 있어서 한계가 존재하였다.

2.1.2 EU GDPR(General Data Protection Regulation, 2018)

EU 개인정보보호지침(Data Protection Directive 95/46/EC)이 '지침'이라는 한계점 때문에 EU 회원국의 적극적인 이행을 이끌어내는데 어려움이 존재하였다. 이에 따라 EU 전역에 걸쳐 개인정보보호에 관한 규율체계가 통일성을 갖지 못해 개인정보의 처리에 있어서 법적 불확실성이 존재하는 상황이 지속되었다. 결국 EU 전체 회원국에 통일적으로 적용될 개인정보 보호법 제정의 움직임이 가시화 되었고, 2012년 GDPR의 초안을 공표하게 되었다. 이후 EU의 입법기관인 유럽의회와 EU 이사회, 그리고 유럽위원회의 3자간 협의를 통해 2016년 5월 4일에 EU공보에 공포되어 동 년 5월 24일부터 발표되었고, 2018년 5월 25일부터 시행되었다[13].

EU GDPR(General Data Protection Regulation)은 총11장 99개조로 구성된 법적 구속력을 가지는 법규범(Regulation) 특히 GDPR은 기업들에게 의무와 제한을 부과하지만 동시에, 개인정보보호 수준 향상으로 인한 기업 및 사회전체에 이익을 제공할 것으로 예측하고 있다[16].

2.2 국내 개인정보보호 법제

2.2.1 개인정보 보호법

「개인정보 보호법」은 개인의 권리와 이를 보호하기 위한 법으로 총 9장 제77개조로 구성되어 2011년 3월 29일 제정되고 동 년 9월 30일부터 시행되었다. 「개인정보 보호법」은 1995년 1월 8일부터 시행되었던 「공공기관의 개인정보보호에 관한 법」을 폐지하고 대체하는 법으로서, 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다[12]. 「개인정보 보호법」은 매년 꾸준하게 개정되며 개인정보주체의 권리를 보장하고 개인정보 처리와 관련된 사회적 흐름에 발맞추어 나아가고자 하였다.

2.2.2 정보통신망 이용촉진 및 정보보호 등에 관한 법률

우리나라의 과거 개인정보 보호체계는 공공부문의 개인정보보호를 위한 「공공기관의 개인정보보호에 관한 법률」과 민간부분 중 특히 「정보통신망법」을 통해 이원적으로 규정되어 있었다. 이후 「공공기관의 개인정보보호에 관한 법률」이 「개인정보 보호법」으로 대체되면서 폐지되었으나, 「정보통신망법」은 여전히 정보통신분야에 개인정보보호와 관련된 상당한 내용을 규정한 채 시행되고 있다.

「정보통신망법」은 1987년 「전산망 보급 확장과 이용촉진에 관한 법률」을 시작으로 2011년 그 명칭이 현재와 같은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로서 전부개정 되었다. 총 10장 제76개조로 구성된 본 법률은 정보통신서비스를 이용하는 자의 개인정보 보호를 위한 다양한 조항을 두고 있다.

2.3 선행연구 분석

GDPR에 대한 선행연구는 많지 않고, 주로 GDPR의 규정 중 일부 조항을 확대 분석하는 연구가 대부분이다. EU GDPR과 관련된 국내 선행연구를 분석하여 소주제별로 다음 <표 1>과 같이 정리하였다.

<표 1> GDPR 관련 선행연구 정리표

소주제	연구자	주요 내용
개인정보 보호책임자	박민정 외 3명 (2018)	GDPR의 DPO 국내 정착 방안을 위해 해외 사례를 분석
바이오정보	정부금 외 3명 (2018)	GDPR을 기반한 바이오정보 보호 법제 개선방안
빅데이터	박노형, 정명현 (2017)	빅데이터 분석기술 활성화를 위한 GDPR 및 개인정보 보호법의 비교분석
영상정보	류기일, 조영임 (2017)	GDPR의 영상정보 보호 규정과 영상정보 내부통제 규제 준수에 대한 연구
인증제도 및 표준	최보미 외 3명 (2018)	개인정보보호 관련 표준 및 인증제도에 대한 현황 파악 및 발전방향 연구
정보이동권	박훤일 (2017)	GDPR의 정보이동권 규정을 국내 도입하기 위한 방안을 연구
프라이버시	조수영 (2018)	개인정보자기결정권과 알권리 등의 보호방안에 대해 고찰
EU 입법동향	권건보 외 3명 (2018)	GDPR 입법 이후 유럽 각국의 개인정보보호 입법동향

분석한 선행연구 정리표를 보면, GDPR이 개인정보보호와 관련된 다양한 주제를 포함하고 있기 때문에, 이와 관련된 여러 선행연구들이 이루어진 것으로 보인다. 그러나 연구들이 공통된 소주제로 이루어진 것이 많지 않고 대부분 개별적인 소주제로 연구가 진행되어 이를 범주화하기 어려웠다. 따라서 각각의 소주제별로 선행연구들을 정리하였다. GDPR이 시행된 지 얼마 되지 않은 시점이기 때문에 관련 된 자료의 축적이 이루어지지 않은 상태여서, 대부분 기존 규정된 법제도에 대한 분석을 하는 연구가 많았다. 그러나 본 연구가 하고자 하는 GDPR과 국내 개인정보보호 관련 법제도의 전반적인 비교분석은 존재하지 않았고, 일부 규정조항을 확대 분석하는 정도가 대부분이었다.

선행연구를 분석한 결과 대부분이 GDPR의 선진적인 규정을 분석하여 국내 관련 법률에 좋은 입법지침으로 삼아야 한다는 점을 강조하였고, 또한 GDPR에 적절히 대응하기 위해 국내 개인정보 보호 법제의 개정 등을 촉구하였다. 그러나 구체적으로 GDPR에 대응하는 전반적인 국내 개인정보보호 관련

법률을 비교분석하는 연구는 일부분이었으며, 그마저도 일부 규정조항만을 비교분석하였다. 결과적으로 본 연구가 진행하고자 하는 GDPR과 국내 개인정보보호 관련 법률의 비교분석은, 기존의 선행연구에서는 찾아볼 수 없었던 전반적이고 총체적인 비교분석 연구라는 점에서 차별성을 갖는다. 특히 GDPR의 모든 규정별 국내의 관련 법률의 조항을 살펴보고 주요 차이점을 기준으로 시사점을 도출한다는 점에서 향후 관련 연구를 진행하고자 하는 연구자들에게나 GDPR 이해 관계자 등에게 선도적인 역할을 할 수 있을 것으로 기대한다.

3. EU GDPR 및 국내 개인정보보호 법제의 비교분석

EU GDPR의 각 규정에 대응하는 사항을 국내 비교대상 법률인 「개인정보 보호법」과 「정보통신망법」에서 찾아 비교분석 하였다. 다만 GDPR의 규정 중 제10장과 제11장은 GDPR의 목적 달성을 위하여 유럽위원회의 위임 입법권 및 이전 지침(95/46/EC) 등과의 관계 등에 대한 사항들을 규정하고 있기에 국내법과 대응하여 비교분석하기 적절하지 않다고 판단하여 제외하였다. 따라서 제1장(일반규정)부터 제9장(특정 정보처리 상황에 관한 규정)까지를 국내 비교대상 법률과 비교분석 하였다.

비교분석 결과 대표적으로 용어 정의·처리활동의 기록·개인정보 영향평가·개인정보 보호담당관·개인정보 역외 이전·감독기관·처벌·법 적용의 예외 사항 등은 GDPR과 마찬가지로 국내법에서도 관련사항을 규정하고 있지만 구체적인 내용에 있어서 차이점을 보인 규정들이다.

먼저 용어 정의에 있어서 GDPR은 가명처리를 정의하였고, 개인의 생체정보를 민감정보 안에 포함시켰다. 반면 국내법에서는 가명처리 개념을 법률 규정으로서 지정하진 않았고, '개인정보 비식별 조치 가이드라인'에 비식별조치의 방법으로서만 명시되어있다. 가명처리의 경우 개인정보의 보호 및 활용을 위한 수단으로서 필요한 개념으로, 관련 사항 도입을 검토할 필요가 있다. 또한 개인의 생체정보의 경우 민감정보 범위 안에 포함되어 있지 않았다. 그러나 개인의 생체정보는 최근 금융·보안 등 사회 곳곳에서 활용되고 있고, 4차 산업혁명에 따라 더욱 그 활용도가 확대될 것이다[8]. 따라서 이러한 생체정보를 보호하기 위해 구체적으로 법률로서 민감정보의 범위 안에 포함시키는 것이 필요하다.

처리활동의 기록의 경우에는 GDPR은 개인정보의 수령인에 대한 정보 및 수탁처리자의 모든 개인정보 처리 활동까지 기록함은 물론, 기술·관리적 안전조치에 대한 설명 등 아주 구체적인 기록까지 서면으로 남기도록 하고 있는 반면, 국내법에서는 개인정보처리자의 개인정보처리시스템에 대한 접속 계정·기록·수행업무 및 접근 권한부여 상태 등을 기록하는데 그치고 있다. 따라서 개인정보처리 활동 전반에 걸친 기록을 하도록 관련 법 개정을 통해 개인정보 유출로 인한 피해사고 대비 시 효율성과 사후 책임 추적성을 용이하게 할 필요가 있다.

개인정보 영향평가의 경우 GDPR은 민간과 공공을 구분하지 않고 중대한 개인정보 처리 전에 반드시 실행하도록 하고 있는데 반면, 국내법에서는 개인정보 영향평가를 공공기관에만 국한하고 있으며, 민간에는 의무사항으로 부과하고 있지 않다. 하지만 이러한 개인정보 영향평가는 사전에 개인정보의 영향과 향후 발생 가능한 침해요인 등을 검토한다는 점에서 민간과 공공부문의 구분 없이 의무사항으로서 부과할 필요가 있으며, 이를 적극적으로 검토해야 할 것이다.

다음 개인정보 보호담당관의 경우 GDPR은 내부 임직원뿐만 아니라 외부의 전문 인력을 채용 가능하도록 하고 있으며, 독립적인 지위 보장과 처벌 면책권을 부여하여 업무 독립성과 지속성을 보장하고 있다. 반면 국내법에서는 내부 임직원만을 채용 대상으로 하고 있으며, 업무의 독립성과 처벌 면책권 등은 부여하고 있지 않다. 결과적으로 국내의 개인정보 보호담당관은 내부 임직원이라는 한계와 독립적인 지위를 보장받지 못하기 때문에, 개인정보 보호담당관으로서의 업무 독립성과 중립성을 기대하기 어렵다. 따라서 올바른 개인정보 보호담당관의 역할을 위해 GDPR의 개인정보 보호담당관(DPO)개념을 적극적으로 도입해야 한다. 특히 이러한 법 개정을 통해서 향후 EU 상대로 사업을 영위할 경우 자연스레 개인정보 보호담당관(DPO)에 관한 규정을 준수하게 되는

효과까지 얻을 수 있으며, 국내 개인정보 보호담당관 제도에 의한 중복 선임 문제도 해결할 수 있을 것이다.

개인정보 역외 이전의 경우 GDPR은 적정성 평가 여부, 적정한 안전조치에 의한 이전, 특정한 상황에 대한 예외적 상황 등을 이전 가능 조건으로 제시하며 세부사항을 아주 구체적으로 정하고 있다. 반면 국내법에서는 개인정보의 국외 이전에 대한 규정이 미흡한데, 「개인정보 보호법」에서는 정보주체의 동의를 요구하고 관련 정보의 통지를 규정하고 있을 뿐이다. 그나마「정보통신망법」에서 국외 이전에 적절한 보호조치를 시행하고 있도록 하고 있다. 따라서 우선적으로 개인정보보호에 있어 일반법인 「개인정보 보호법」에 개인정보 국외 이전과 관련된 보다 구체적인 조항이 신설되어야 할 것으로 보이며, 「정보통신망법」과의 규정 통일을 통해 법적 근거 판단의 혼란을 최소화하고 국외 이전되는 개인정보의 적절한 보호조치를 취해야만 할 것이다.

다음 감독기관의 경우 GDPR은 개인의 기본권과 자유를 보호하고 유럽연합 역내에서 개인정보의 자유로운 이전을 촉진하기 위해 GDPR의 규정 준수 감독과 더불어서 개인정보 보호 인증 사업·개인정보 영향평가·법률 및 행정 조치 자문·인식 제고 교육 등 개인정보보호와 관련된 전반적 업무를 총괄하는 개인정보보호 감독기관을 설립하도록 하고 있다. 특히 이러한 감독기관은 본 규정에 따른 직무를 수행하고 권한을 행사하는데 있어서 완전한 독립성을 가지도록 하고 있으며, 외부의 직간접적인 영향을 받지 않고, 다른 어떤 이로부터의 지시를 구하거나 받지 않도록 하고 있다. 반면 국내법에서는 개인정보 감독기관으로서 별도의 규정은 존재하지 않았고, 각각의 규정에 일부분으로서 「개인정보 보호법」은 행정안전부, 「정보통신망법」은 방송통신위원회를 감독기관의 성격으로 위임하고 있었다. 또한 현재 「개인정보 보호법」에서 규정하고 있는 개인정보보호위원회는 그 권한과 지위가 실질적으로 미흡한 상황이었다. 국내 법률에서 감독기관으로서의 구체적인 업무에 있어서는 GDPR과 큰 차이가 존재하지는 않았지만, GDPR은 중앙행정기구로서의 독립된 감독기관 설립을 의무로 하여 지위나 독립성 측면에서 우리나라와 차이를 보였다. 더불어서 실제적인 감독기관이「개인정보 보호법」과 「정보통신망법」에 의해 각각 행정안전부와 방송통신위원회로 이원화되어 있기 때문에 관련 업무의 중복을 배제하기 어렵고, 효율성을 도모하기 힘든 상황이다. 따라서 감독기관의 경우 「개인정보 보호법」에 그 근거 법령을 두고, 독립적인 중앙행정기구를 설립하거나 개인정보보호위원회로 이관하여 개인정보보호 전반에 걸친 감독 및 관리 등을 담당하도록 해야 할 것이다.

처벌과 관련하여서 GDPR은 최대 2천만유로 또는 연간 전 세계 매출액 4%중 높은 것을 부과하도록 하고 있는 반면, 「개인정보 보호법」과 「정보통신망법」은 과태료 5천만원이 최대이며 예외적으로 「정보통신망법」에서 과징금의 개념으로 위반행위와 관련된 매출액의 최대 3% 까지 부과 가능함을 명시하고 있을 뿐이다. 이러한 낮은 수위의 과태료 및 과징금은 사업자로 하여금 법에 대한 경각심을 일깨워주기 부족하며, 법 위반 억제성의 효과를 달성하기도 힘들 것이다. 따라서 개인정보보호 관련 법률의 위반 시 강력한 처벌 및 벌금 등을 부과하여 개인정보처리자로 하여금 법에 대한 엄격성을 일깨워주어야 할 것이다.

마지막으로 법 적용의 예외 사항으로서 GDPR은 특정한 정보처리상황에 관한 규정을 명시하고 있다. 그 내용으로는 언론·학술·예술·문학·고용환경·공익·역사적 연구·통계적 목적·종교 등 특정한 상황에서의 정보처리의 경우 GDPR과의 적절한 균형과 조화를 통해 일부 규정의 적용을 아니 할 수 있도록 하는 것이다. 이러한 규정은 적절한 안전조치가 기반 되었을 때 다양한 분야에서 폭넓게 특수한 상황을 인정하고 GDPR의 규정을 적용받지 않을 수 있도록 하여 개인정보의 적극적인 활용을 보장하고 있다. 반면 우리나라의 경우 법 적용의 예외 사항이 매우 소극적인데, 공공과 국가안전보장 등의 목적, 언론·종교·정당이 각각 고유 목적을 달성하기 위한 상황, 친목 도모를 위한 단체 등에서만 해당된다. 이처럼 확연하게 GDPR과 국내법은 법 적용의 예외 사항에서 차이를 보이고 있으며, 이는 곧 우리나라의 경우 다양한 분야에 개인정보 활용에 있어서 제한이 있음을 알 수 있는 것이다. 다만, 무조건적으로 개인정보의 활용만

을 강조해서는 아니 될 것이며, 반드시 적절한 안전 조치를 기반하고 관련한 법률적 근거를 통해 개인정보 활용을 위한 법률 적용의 예외 사항에서의 확대가 고려되어져야 할 것이다.

이렇듯 GDPR과 국내법에서 비슷한 규정 조항들이 존재하였지만 구체적인 내용에서는 큰 차이점을 보이고 있었다.

반면 GDPR에서는 규정하고 있지만 국내법에서는 아예 관련사항을 규정하고 있지 않은 내용도 있었는데, 법률 역외 적용·개인정보 이전권·프로파일링 등 자동화된 의사결정의 거부권·역내 대리인 지정이 바로 그것이다.

법률 역외 적용의 경우 GDPR은 EU 역내에 사업장을 운영하고 있지 않아도, EU 정보주체에게 사업을 영위하며 개인정보를 처리하는 경우 법 적용 대상으로 삼았다. 따라서 사업자 등은 EU역내에 사업장이 없어도, EU 정보주체의 개인정보 처리를 기반 할 경우 GDPR의 법 적용 대상이 되기 때문에 GDPR 준수를 위한 노력을 해야 한다. 특히 최근의 글로벌 정보사회 환경 속에서는 온라인상의 사업도 활발하기 때문에, 반드시 물리적 사업장이 필요하지 않을 수 있다. 따라서 법률의 역외 적용은 오늘날의 사회 환경에서는 반드시 필요한 부분이라고 할 수 있다. 그러나 현재 국내의 개인정보보호 관련 법률은 역외 적용을 규정하지 않아 국내에서 사업을 영위하지만, 사업장이 존재하지 않는 국외의 사업자에 대한 법 적용이 불가능한 상황이다. 이는 국내에 사업장이 존재하지 않는 국외의 사업자에게 법적 강제성을 부과할 수 없고, 이와 관련된 국내의 정보주체의 기본권 및 권리의 침해도 발생 가능하다. 따라서 국내에 사업장을 두고 있지 않은 국외의 사업자 등에게도 국내의 개인정보보호 관련 법률이 적용될 수 있도록 역외 적용 규정을 신설할 필요가 있으며, 이를 통해 국외 사업자의 책임성 강화와 국내 정보주체의 기본권 및 권리를 보호할 필요가 있다.

개인정보 이전권의 경우 정보주체로 하여금 자신의 개인정보를 여러 다른 서비스에 걸쳐 재사용할 수 있도록 개인정보처리자 등에게 본인의 개인정보 이전을 요구할 수 있는 권리이다. 이러한 개인정보 이전권은 정보주체로 하여금 반복되는 정보제공 등의 비효율성을 제거할 수 있고, 편리한 개인정보 이전을 통해 개인정보 활용의 확대를 도모할 수도 있다. 특히 본 규정은 개인정보의 활용 측면에서 정보주체의 자발적인 요청을 근거로 하기 때문에 개인정보 활용에 있어서 상당히 용이하다. 따라서 우리 역시 적절한 보호조치를 기반 한 개인정보 이전권과 같은 개념의 도입을 검토 할 필요가 있다.

다음 프로파일링 등 자동화된 의사결정의 거부권은 자동화된 개인정보처리시스템 등으로 일방적이고 단편적인 방법에 의한 정보주체의 이익 침해를 방지하고자 정보주체에게 부여한 권리이다. 특히 오늘날은 인공지능, 빅데이터 등의 발전 및 이용으로 이러한 자동화된 의사결정 처리 시스템이 활발해질 수 있기 때문에, 정보주체의 기본권 및 권리 침해가 발생 가능하다. 따라서 이러한 폐해를 방지하기 위해 관련 규정의 도입을 고려해야 한다.

마지막 역내 대리인의 경우 국내법에서는 관련 사항이 존재 하지 않았는데, 최근「정보통신망법」의 개정을 통해, 2019년 3월 19일부터 국내에 주소 또는 영업소가 없는 정보통신서비스를 이용한 사업자 등에게 국내 대리인을 지정하도록 하였다. 이는 결국 상기 서술한 법 역외 적용의 미비점을 보완하는 내용으로 국내 정보주체의 권리를 보호하고자 하였다는 점에서 긍정적으로 평가할 수 있다.

이처럼 GDPR은 개인정보보호와 관련된 최신동향이 반영되고 개인정보주체의 기본권 및 권리보호를 위한 법적 성격과 다양한 규정을 포함하고 있다는 점에서, 개인정보 보호법으로서의 GDPR 가치를 확인할 수 있었고, 이를 통해 국내 개인정보보호 법제를 점검하고, 시사점을 도출해 낼 수 있었다.

4. 결 론

세계는 개인정보보호를 위한 법과 제도, 기술 등을 강화하고 있는 추세이다. EU 역시 이에 발맞추어 기존의 개인정보보호지침을 대체하는 GDPR을 제정하고 2018년 5월 25일부터 시행하고 있다. GDPR은 EU 회원국 모두에게 직접적으로 적용되고, 법적 구속력을 지닌다. 또한 GDPR은 2012년부터 4년간의 논의를 거쳐 2016년에 완성되었기에, EU의 신중함과

노력이 기해지는 것은 물론이고 개인정보보호와 관련된 최신동향이 반영되었다. 따라서 이를 분석하는 것은 GDPR을 이해하고, 국내 개인정보보호 법제의 좋은 입법 참고 자료로서 활용할 수 있는 가치 있는 일이다.

이에 본 연구는 개인정보보호법으로서의 GDPR의 법적 위상과 가치가 상당하다는 판단아래, 이를 국내법과 비교분석해봄으로써 국내의 개인정보보호 관련 법률의 점검 및 개선점 등을 도출해내고자 하였다.

비교대상 법으로서 개인정보보호와 관련된 일반법인 「개인정보 보호법」과 정보통신망서비스 제공자 및 이용자에게 적용되는 「정보통신망법」을 선정하였다. 특히 「정보통신망법」 경우 정보통신망 이용자의 개인정보보호에 관한 내용을 상당 부분 규정하고 있고 관련 내용이 일반법인 「개인정보 보호법 」에 우선하여 적용된다. 또한 법 적용 대상이 정보통신망을 이용하여 서비스를 제공하는 사업자 대부분이 해당된다는 점에서 비교대상 법으로서 반드시 포함시킬 필요가 있었다.

본 연구의 비교분석 결과로, GDPR과 국내 비교대상 법률은 민감정보 정의·처리활동의 기록·개인정보 영향평가·개인정보 보호담당관·개인정보 역외 이전·감독기관·처벌·법 적용 예외 사항 등에서 규정상의 큰 차이를 보이고 있었으며, 법률 역외 적용·개인정보 이전권·프로파일링 거부권·역내 대리인 지정 등은 국내 법률의 규정에 아예 존재하지 않는 내용이었다.

이러한 규정상의 차이 이외에도 GDPR은 국내법과 근본적으로 법적 성격의 차이를 보이고 있었다. GDPR의 경우 개인정보의 보호와 활용적 측면 모두를 균형적으로 다루며, 보호해야 할 개념이나 대상에 있어서 구체성을 보였다. 또한 개인정보 처리보안 등에 있어서의 구체적인 방안은 개인정보처리자 등에게 자율적으로 위임하고, 이후 이를 증명하도록 하였다. 따라서 개인정보처리자 등은 자율적이고 주도적인 개인정보보호 체계의 확립 및 발전을 이끌어 낼 수 있는 선순환적인 구조를 제공한다. 반면 국내법은 개인정보의 보호 측면에만 집중하는 경향을 보였으며, 보호 방안에 있어서 구체성을 보이고 있었다. 예컨대 「개인정보보호법」의 '개인정보의 안전성 확보조치 기준', 「정보통신망법」의 '개인정보의 기술적·관리적 보호조치 기준' 등이 해당된다. 이러한 규정들은 결과적으로 개인정보처리자로 하여금 법률상 규정 된 내용만 이행하도록 하여 수동적인 자세를 갖게 한다. 결국 국내 개인정보처리자 등은 자율적이고 주도적인 개인정보보호 체계 확립 및 발전에 있어 어려움이 존재하게 되는 것이다. 따라서 국내 개인정보보호 관련 법률 역시 GDPR과 같이 개인정보처리자 등이 책임의식 및 수준 발전을 함양할 수 있는 법률적 환경을 제공하는 패러다임의 전환이 필요하다. 이를 통해 국내 개인정보보호 수준의 향상을 도모해야 할 것이다.

이처럼 GDPR과 국내 개인정보보호 관련 법률은 법적 성격과 세부적인 규정 내용에 있어서 많은 차이를 보이고 있었다. 또한 그러한 차이점이 개인정보보호 관련 법제의 개선에 중요한 부분으로 작용 할 수 있을 것으로 보였기 때문에 GDPR을 개인정보보호 법제의 참고 자료로 활용할 가치는 충분하였다. 따라서 본 연구가 비교분석한 결과물과 법적 개선점 제언 등을 통해 국내의 개인정보보호 법제의 전체적인 점검 및 수준 향상을 도모하는데 이바지할 수 있을 것으로 기대한다.

다만, 본 연구는 GDPR과 비교분석하는 대상 법률로서 국내 주요 개인정보보호 법률인 「개인정보 보호법」과 「정보통신망법」 만을 채택하여 연구를 진행하였기 때문에, 이외의 개인정보보호 관련 법률을 폭 넓게 다루지 못하였다는 한계를 지닌다. 또한 GDPR의 전반적인 내용을 국내법과 비교분석 하고 이에 대한 국내법의 개선점을 제언하였기 때문에 큰 틀에서 법 내용 전반을 다뤘다는 점은 긍정적이나, 각각의 규정상의 차이를 국내에 도입할 시 구체적 방안과 발생가능한 문제점이나 해결방안 등에 대한 구체성이 다소 부족한 부분이 존재하였다. 그러나 아직 GDPR이 시행된 지 얼마 지나지 않아 관련한 사례나 자료 축적이 많지 않기 때문에 구체적인 법적 개선점이나 도입 방안 등을 제시하기 어려운 부분이 있었다. 따라서 향후연구과제로서 GDPR 및 국내 개인정보보호 관련 연구와 자료 등이 축적된다면, 이를 토대로 법적 개선점 및 도입 방안 등의 구체적 방안에 대해 연구할 필요가 있을 것으로 보인다.

<표 2> GDPR과 「개인정보 보호법」 및 「정보통신망법」 주요 규정 차이 비교

	GDPR	개인정보 보호법	정보통신망법
역외 적용	제3조(지리적 범위)	×	×
용어 정의	제4조(정의)	제2조(정의)	제2조(정의)
개인정보 이전권	제20조(개인정보 이전권)	×	×
자동화된 의사결정 거부권	제22조(프로파일링 등 자동화된 의사결정)	×	×
역내 대리인	제27조(EU 내에 설립되지 않은 사업자의 대리인 지정)	×	제32조의5(국내대리인의 지정) 〔시행일 : 2019.3.19.〕
처리활동 기록	제30조(처리활동의 기록)	제29조(안전조치의무) 동법 시행령 제30조(개인정보의 안전성 확보 조치)	제28조(개인정보의 보호조치) 동법 시행령 제15조(개인정보 보호조치)
개인정보보호 영향평가	제35조(개인정보보호 영향평가) 제36조(사전 자문)	제33조(개인정보 영향평가) 동법 시행령 제38조에 따른 영향평가 고시	×
개인정보 보호담당관	제37조(개인정보보호 담당관의 지정) ~ 제39조(개인정보보호 담당관의 업무)	제31조(개인정보 보호책임자의 지정) 동법 시행령 제32조(개인정보 보호책임자의 업무 및 지정요건)	제27조(개인정보 보호책임자 지정) 동법 시행령 제13조(개인정보 보호책임자의 자격요건)
개인정보 역외 이전	제44조(이전을 위한 통칙) ~ 제49조(특정 상황에 대한 적용의 일부 제외)	제14조(국제협력) 제17조 제3항(개인정보 제공)	제63조(국외 이전 개인정보 보호) 제63조의2(상호주의) 〔시행일 : 2019.3.19.〕 동법 시행령 제67조(개인정보 국외 이전시 보호조치)
감독기관	제51조(감독기관) ~ 제62조(감독기관의 공동 작업)	·행정안전부 ·개인정보 보호위원회 (제7조 ~ 제11조) ·개인정보 분쟁조정위원회 (제40조 ~ 제50조)	·방송통신위원회 ·한국인터넷진흥원(제52조)
처벌	제83조(행정 과태료 부과에 관한 일반조건) 제84조(처벌)	제34조의2(과징금의 부과) 제71조(벌칙) ~ 제76조(과태료 적용의 특례)	제64조의3(과징금의 부과) 제70조(벌칙) ~ 제75조의2(몰수·추징)
특정 정보처리 상황	제85조(개인정보 처리 및 표현과 정보의 자유) ~ 제91조(교회 및 종교 단체의 현행 정보보호 규정)	제18조(개인정보 목적 외 이용·제공 제한) 제58조(적용의 일부 제외)	×

참고문헌

[1] 권건보, 이한주, 김일환, “EU GDPR 제정 과정 및 그 이후 입법동향에 관한 연구”, 미국헌법연구, 제29권, 제1호, 1-38, 2018.

[2] 류기일, 조영임, “GDPR의 영상정보 보호 규정과 영상정보 내부통제 규제 준수에 대한 연구”, 한국컴퓨터정보학회논문지, 제22권, 제6호, 41-48, 2017.

[3] 문재완, “유럽연합(EU) 개인정보보호법의 특징과 최근 발전”, 외법논집, 제40권, 제1호, 1-18, 2016.

[4] 박노형, 정명현, “빅데이터 분석기술 활성화를 위한 개인정보보호법의 개선 방안 - EU GDPR과의 비교 분석을 중심으로 -”, 고려법학, 제85권, 1-39, 2017.

[5] 박민정, 채상미, 이명준, “General Data Protection Regulation(GDPR) 시행에 따른 정보보호담당관(DPO)의 국내 정착 방안에 대한 연구”, 한국통신학회논문지, 제43권, 제2호, 427-438, 2018.

[6] 박훤일, “정보이동권의 국내 도입 방안 - EU GDPR의 관련 규정을 중심으로 -”, 경희법학, 제52권, 제3호, 211-232, 2017.

[7] 방송통신위원회, 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서, 2012.

[8] 정부금, 권헌영, 박혜숙, 임종인, “글로벌 바이오정보 프라이버시 논점 분석을 기반으로 한 바이오정보 보호 가이드라인 개선 방안”, 융합보안논문지, 제18권, 제3호, 87-94, 2018.

[9] 정부금, 권헌영, 박혜숙, 임종인, “바이오정보 활용 서비스 현황 및 GDPR 사례를 통한 바이오정보보호 법제 개선방안”, 한국통신학회논문지, 제43권, 제1호, 201-208, 2018.

[10] 조수영, “개인정보보호법과 EU의 GDPR에서의 프라이버시 보호에 관한 연구”, 법학논고, 제61권, 117-148, 2018.

[11] 최보미, 채상미, 김민균, 강연정, “GDPR 환경에서 국내 개인정보보호 관련 인증제도 및 표준 발전방향에 대한 연구”, 한국통신학회논문지, 제43권, 제2호, 416-426, 2018.

[12] 한세진, “개인정보보호법이 금융권에 미치는 영향과 문제점에 관한 고찰”, 융합보안논문지, 제13권, 제1호, 31-36, 2013.

[13] 함인선, “EU의 2016년 일반정보보호규칙(GDPR)의 제정과 그 시사점”, 법학논총, 제36권, 제3호, 411-453, 2016.

[14] 홍선기, “일반개인정보보호규정(GDPR) 발효에 따른 독일 개인정보보호법제의 입법동향 및 시사점”. 정보법학, 제22권, 제1호, 175-202, 2018.

[15] Beckett, P, “GDPR compliance: your tech department's next big opportunity”, COMPUTER FRAUD AND SECURITY, Vol 2017, No 5, pp 9-13, 2017.

[16] Krystlik, J, “With GDPR, preparation is everything”, COMPUTER FRAUD AND SECURITY, Vol 2017, No 6, pp 5-8, 2017.

〔저자소개〕

김 성 현 (Sung-hyun Kim)

2017년 ~ 현재 중앙대학교 산업융합보안학과 석사과정

email : kimsuhy89@gmail.com

이 창 무 (Chang-moo Lee)

2002년 뉴욕시립대 형사사법학 박사

2003년 ~ 2014년 한남대학교 경찰행정학과 교수

2014년 ~ 현재 중앙대학교 산업보안학과 교수

email : cmlee@cau.ac.kr